UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/878,536	06/11/2001	Paul Patrick	BEAS-01084US0	4065

23910 7590 11/01/2007

FLIESLER MEYER LLP
650 CALIFORNIA STREET
14TH FLOOR
SAN FRANCISCO, CA 94108

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
11/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/878,536	PATRICK, PAUL	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-7,10-12,18,19,21-24,27-29,35-39,42 and 43* is/are pending in the application.

4a) Of the above claim(s) *35-39* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-7,10-12,18,19,21-24,27-29,42 and 43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/07 and 10/07*.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. *20071026*.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/20/07 has been entered.

Claims 1-2, 5-7, 10-12, 18-19, 21-24, 27-29, 42-43 were examined. Applicant's amendments and arguments with respect to the examined claims were fully noted, but are moot in view of new rejections presented below.

Information Disclosure Statement

Documents listed in the IDS's submitted on 8/20/07 and 10/18/07 have been considered.

Claim Objections

Claims 1, 5, 18, 23, and 42-43 are objected to because of the following informalities:

1. As per claim 1:
    a. "an application container" in line 3 should be "the application container.
    b. "a client" in line 6 should be "the client".
    c. "context information" in line 14 should be "the context information".
    d. "can be" as recited in line 13 should be "is" as per the interview held between the examiner and applicant's representative on 10/18/07.

2. In claim 5, "can determine" should be "determines" as per the interview held between the examiner and applicant's representative on 10/18/07.
3. As per claim 18:
    a. "Application Container" in line 2 should be "application container".
    b. Line 3 should recite "the application container" instead of "an application container".
    c. Line 7 should recite "the access request and the callback handler" instead of "an access request and a callback handler".
    d. Line 8 should recite "the access request" instead of "an access request".
    e. Line 13 should recite "the context information".
    f. In line 20, "can be" should instead be "is" as per the interview held between the examiner and applicant's representative on 10/18/07.
4. In claim 23, "transferring, via an access controller, the access request..." should be recited, note the commas added.
5. In claims 42 and 43, "the protected resource" should be recited instead of "a protected resource".
6. Note as per instructions by applicant's representative, in examining the claims, the examiner examined them with respect to the above corrections being made to the claims. Applicant should, however, make formal corrections in response to this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Note that with respect to the present application, it was determined that a person of ordinary skill in the art is someone having at least a BS in Computer Science/Engineering and is experienced in the practical application of computer/network security concepts especially using object-oriented programming languages, like Java (or someone with equivalent industry experience).

Claims 1-2, 4, 18-19, 21, and 42-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sampson et al (US 6,339,423) in view of Sharma (US 7,089,584) further in view of Barkley (US 6,088,679).

Claims 1 and 18:

As per claim 1, Sampson discloses:

1. The application container (i.e. Fig 2, servers 205), which provides services for a protected resource (i.e. Fig 2, servers, 240, 260, and 280 and resources 248-249, 268-269, and 288-289), wherein the application container delegates authorization decisions to a security service (i.e. Fig 2, access controller 220) by passing an access request and to the security service when the application container receives the access request for a protected resource from the client

(col 4, lines 35-40 and 57-66 and col 5, lines 14-23). *Note that in the cited section, server 205 receives an access request to a resource from a client via a browser request. The server 205 forwards the request and to access controller 220, which authenticates the user and decides whether or not to grant the user's request.*

2. Context information, wherein the context information comprises one or more parameter values describing the access request, identity of the protected resource, and profile information describing the client (col 4, lines 57-66 and col 7, lines 23-50).

3. The security service (i.e. access controller 220) for making a decision to permit or deny the access request (col 4, lines 57-66), wherein a plurality of security plug-ins (i.e. Fig 2, domain agents 242, 262, and 282 and token server 208 and col 6, lines 47-55) that implements an access decision interface are plugged into the security service (Fig 2, item 220 and col 5, lines 14-23), and wherein depending on output from each security plug-in the security service determines entitlements for the client to use with the protected resource (col 6, line 57-col8, line 59). *Each of items 242, 262, 282, and 208 are plug-ins which are plugged into access controller 220. In portions of columns 6-8 cited, it is discussed that each of these plug-ins interact with each other to determine whether or not to approve a client's request to a resource. The decision is dependent on the output from each of the plug-ins and the resulting access control cookies determines the privileges/entitlements of the client.*

4. The security service is located at a first computer, and said protected resource is located either at the same first computer or at a second computer (col 6, lines 21-35).

Sampson does not explicitly disclose:

1. The application container passing a callback handler to the security service.
2. Wherein the plurality of security plug-ins use the callback handler to request the context information from the application container for the access request, and wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles is computed dynamically at runtime.

However, Sharma discloses of an application container (i.e. application server) passing a callback handler to a security service (i.e. JAAS module for Kerberos or EIS specific JAAS module), wherein the security service's plug-in uses the callback handler to request context information from the application container for the access request (col 19, lines 4-14 and 39-43 and col 20, lines 13-15 and 32-53). Note that the portions of Sharma cited discuss two different embodiments of Sharma. In both embodiments, JAAS is used in the security architecture to authenticate the user and enforce access controls on the users. The application container passes a callback handler to a JAAS module which controls authentication in Sharma's invention. The JAAS module when it needs more information concerning the context of the request uses the callback handler

that was passed to it to obtain the needed context information. Note that the JAAS modules are plug-in's (co 16, lines 60-67). In both the embodiments of Sharma's invention, the only difference is the type of JAAS module utilized to perform the authentication; one uses Kerberos and the other uses an EIS specific JAAS module.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to incorporate Sharma's teachings within Sampson's invention by utilizing JAAS plug-ins within Sampson's security service such that when Sampson's security service passes an access request to the security service, it also passes a callback handler, wherein the [JAAS] plug-ins of the security service would then use the callback handler to request any needed context information from the application container for the access request. One of ordinary skill would have been motivated incorporate Sharma's teachings because use of JAAS plug-in modules for security purposes would provide flexibility to Sampson's invention since the JAAS framework is based on the concept of configurable authenticators and would allow applications to remain independent form the underlying application and thus authenticators could be replaced as needed to meet the security requirements of different resources without having to modify or recompile existing applications.

Sharma also does not explicitly disclose wherein the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles is computed dynamically at runtime. However, Barkley discloses a method of controlling access to computer systems called role-based access control (RBAC) in which roles for a client is determined and wherein association of the client to roles is

computed dynamically at runtime (col 2, lines 50-60; col 3, lines 20-24; col 4, lines 17-22; and col 6, lines 22-62).

In light of this, it would have been obvious to one of ordinary skill in the art to further modify Sampson's invention to use RBAC so that the plurality of security plug-ins determine roles for which the client is entitled, and wherein association of the client to roles is computed dynamically at runtime. One skilled in the art would have been motivated to utilize RBAC in Sampson's invention because RBAC reduces administrative cost and complexity as compared to other access control mechanisms (Barkley: col 2, lines 53-56).

Claim 18 is directed towards a method implemented using the security system of claim 1 and thus is rejected for substantially the same reasons as claim 1. Note that Sampson also discloses communicating a permitted access request to the protected resource as recited in claim 18 (col 8, lines 52-59).

Claims 2 and 19:

Sampson, Sharma, and Barkley render obvious all the limitations as recited in claims 1 and 18. In addition, Sharma further makes obvious the limitation wherein the application container of claim 1 reads an application deployment description and registers the application deployment description within the security service (col 6, lines 53-62; col 8, line 62-col 9, line 2; col 10, lines 21-24; and col 18, lines 1-12).

Claims 4 and 21:

Sampson, Sharma, and Barkley render obvious all the limitations as recited in claims 2 and 19. In addition, Sampson and Sharma further makes obvious the limitation

of wherein the application container is a Web Application container (Sampson: Fig 2 and Sharma: col 7, lines 35-49). Enterprise Java Bean (EJB) and servlet containers are Web applications. The resources of servers 205 of Sampson's invention as seen in Figure 2 are accessed using a web browser, thus the applications located on these servers are web applications, which would make servers 205 Web Application containers.

Claims 42 and 43:

Sampson, Sharma, and Barkley render obvious all the limitations as recited in claims 1 and 18. Barkley further discloses wherein computation of a dynamic role occurs immediately before an authorization decision for the protected resource (col 4, lines 17-22 and col 6, lines 22-52

Claims 5-7, 10-11, 22-24, and 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sampson et al (US 6,339,423) in view of Sharma (US 7,089,584) further in view of Barkley (US 6,088,679) and further in view of Hummel, Jr. et al (US 6,584,454).

Claims 5 and 22:

Sampson, Sharma, and Barkley render obvious all the limitations as recited in claims 1 and 18. Sampson does not explicitly disclose the following limitation, however it is disclosed by Hummel: wherein each of the plurality of security plug-ins determines a

contributory decision to permit, deny, or abstain from the access request (col 3, lines 4-20).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to incorporate Hummel's teachings within the modified invention of Sampson. One skilled would have been motivated to do so because it would provide for a system that load balances the decision for resource access, which would allow for decisions to be reached faster, resulting in faster access to resources.

Claims 6 and 23:

Sampson, Sharma, Barkley, and Hummel render obvious all the limitations as recited in claims 5 and 23. Hummel further discloses wherein the security service further includes an access controller for transferring the access request to the plurality of security plug-ins, and for combining the contributory decisions into an overall decision by the security service to permit or deny the access request (col 3, lines 39-60).

Claims 7 and 24:

Sampson, Sharma, Barkley, and Hummel render obvious all the limitations as recited in claims 5 and 23. Hummel further discloses wherein one or more of the security plug-ins represent a business function related authorization policy (col 4, lines 50-60).

Claims 10 and 27:

Sampson, Sharma, Barkley, and Hummel render obvious all the limitations as recited in claims 5 and 23. Hummel further discloses wherein a deny or abstain by any

one of the security plug-ins causes the security services to deny the access request (col 12, lines 25-32).

Claims 11 and 28:

Sampson, Sharma, Barkley, and Hummel render obvious all the limitations as recited in claims 5 and 23. Hummel further discloses wherein an abstain by any one of the plurality of security plug-ins does not cause the security service to deny the access request (col 3, lines 6-11). Note that if the resource/application is open, then the agency model makes a decision to allow access while the policy server is not consulted about the access thereby abstaining from an access decision. This makes obvious that if a plug-in does not have anything to contribute with respect to an access request, it abstaining from contributing to the decision about the request should not cause a deny in the access request.

Claims 12 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sampson et al (US 6,339,423) in view of Sharma (US 7,089,584) further in view of Barkley (US 6,088,679) and further in view of Hummel, Jr. et al (US 6,584,454) and further in view of Wiederhold (US 6,226,745).

Claims 12 and 29:

Sampson, Sharma, Barkley, and Hummel render obvious all the limitations as recited in claims 5 and 23. Sampson does not explicitly disclose wherein the security service further includes security plug-ins that implement an audit interface for auditing

the determinations of the plurality of access requests. However, this limitation is disclosed by Wiederhold (col 5, last paragraph and col 6, lines 1-2).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Sampson's invention according to the limitations recited in claims 12 and 29. One skilled would have been motivated to do so because it would allow policies that are too stringent or too liberal to be recognized and the system can be adjusted accordingly (Wiederhold: col 3, lines 61-67).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100